IN THE CLAIMS

Please amend the claims as follows:

1-25. (Canceled)

26. (Original) A method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

a public-key management apparatus and the first apparatus exchange key information used for performing encrypted communication, and the public-key management apparatus and the first apparatus perform mutual authentication so that a first encrypted communication channel is established;

the public-key management apparatus and the second apparatus exchange key information used for encrypted communication, and the public-key management apparatus and the second apparatus perform mutual authentication so that a second encrypted communication channel is established;

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel;

the public-key management apparatus stores the received public-key in its storage device, and the second apparatus obtains the public-key from the public-key management apparatus via the second encrypted communication channel so that a third encrypted communication channel using the public-key between the first apparatus and the second apparatus is established.

27-29. (Canceled)

30. (Original) A public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel;

a part for receiving a public-key of the first apparatus via the first encrypted communication channel;

a part for storing the received public-key in its storage device; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus.

31. (Original) The public-key management apparatus as claimed in claim 30, wherein the public-key management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys.

32. (Previously Presented) The public-key management apparatus as claimed in claim 30, the public-key management apparatus further comprising:

a part for performing message communications between the first apparatus and the public-key management apparatus and between the second apparatus and the public-key management apparatus by using Session Initiation Protocol.

33. (Canceled)

34. (Currently Amended) A non-transitory computer-readable medium including a computer program, which when executed by a computer causes the ~~for causing a~~ computer to function as a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the computer program comprising:

program code ~~means~~ for exchanging key information used for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

program code ~~means~~ for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel;

program code ~~means~~ for receiving a public-key of the first apparatus via the first encrypted communication channel;

program code ~~means~~ for storing the received public-key in a storage device; and

program code ~~means~~ for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus.

35. (Original) A session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and storing a name of the first apparatus and identification information of the first

encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

a part for receiving a message including a name of the first apparatus via the first encrypted communication channel;

a part for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel; and

a part for sending the message to the second apparatus via the second encrypted communication channel.

36. (Original) The session management apparatus as claimed in claim 35, wherein, if the session management apparatus determines that the name of the first apparatus included in the message is not correct, the session management apparatus sends an error message to the first apparatus.

37. (Original) A session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

a part for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel.

38. (Original) The session management apparatus as claimed in claim 37, wherein the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the first header by comparing an address included in the first header and an address of the first apparatus.

39. (Original) The session management apparatus as claimed in claim 35, wherein the message is based on Session Initiation Protocol.

40. (Original) A method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and the session management apparatus stores a name of the first apparatus and identification information of the first encrypted

communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

the session management apparatus and the second apparatus performs mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

the first apparatus sends a message including a name of the first apparatus via the first encrypted communication channel to the session management apparatus;

the session management apparatus determines whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel; and

the session management apparatus sends the message to the second apparatus via the second encrypted communication channel.

41. (Original) A method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

the session management apparatus and the second apparatus perform mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

the session management apparatus adds a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sends the message to the second apparatus via the second encrypted communication channel.

42. (Currently Amended) A non-transitory computer-readable medium including a computer program, which when executed by a computer causes the ~~for causing a~~ computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code ~~means~~ for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

program code ~~means~~ for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

program code ~~means~~ for receiving a message including a name of the first apparatus via the first encrypted communication channel;

program code ~~means~~ for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel; and

program code ~~means~~ for sending the message to the second apparatus via the second encrypted communication channel.

43. (Currently Amended) A non-transitory computer-readable medium including a computer program, which when executed by a computer causes the ~~for causing a~~ computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code ~~means~~ for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

program code ~~means~~ for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

program code ~~means~~ for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

program code ~~means~~ for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel.

44. (New) A method for establishing an encrypted communication channel between a first apparatus and a second apparatus, and performing communication between the second apparatus and a third apparatus using the encrypted communication channel, comprising:

a first step of exchanging key information for encrypted communication and performing mutual authentication between a session management apparatus and the second

apparatus so as to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

a second step in which the first apparatus is accessed by the third apparatus;

a third step of exchanging key information for encrypted communication and performing mutual authentication between the session management apparatus and the first apparatus so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

a fourth step in which the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a connection request message destined for the second apparatus including key information used for encrypted communication between the first apparatus and the second apparatus, and the session management apparatus sends the connection request message to the second apparatus via the second encrypted communication channel;

a fifth step in which the second apparatus sends, to the session management apparatus via the second encrypted communication channel, a response message including key information used for encrypted communication between the first apparatus and the second apparatus in response to receiving the connection request message, and the session management apparatus sends the response message to the first apparatus via the first encrypted communication channel;

a sixth step in which the. first apparatus receives data from the second apparatus via the encrypted communication channel established between the first apparatus and the second apparatus, and sends the data to the third apparatus,

wherein the first apparatus is provided with a table including at least one connection destination permitted for the third apparatus, and the first apparatus sends information of the at least one connection destination to the third apparatus in response to receiving access from

the third apparatus, and receives a connection destination from the third apparatus so as to send the connection request message destined for the second apparatus to the session management apparatus in the fourth step based on the connection destination received from the third apparatus.

45. (New) A method for establishing an encrypted communication channel between a first apparatus and a second apparatus, and performing communication between the second apparatus and a third apparatus using the encrypted communication channel, comprising:

a first step of exchanging key information for encrypted communication and performing mutual authentication between a session management apparatus and the first apparatus so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

a second step of exchanging key information for encrypted communication and performing mutual authentication between the session management apparatus and the second apparatus so as to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

a third step in which the first apparatus is accessed by the third apparatus;

a fourth step in which the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a connection request message destined for the second apparatus including key information used for encrypted communication between the first apparatus and the second apparatus, and the session management apparatus sends the connection request message to the second apparatus via the second encrypted communication channel;

a fifth step in which the second apparatus sends, to the session management apparatus via the second encrypted communication channel, a response message including key

information used for encrypted communication between the first apparatus and the second apparatus in response to receiving the connection request message, and the session management apparatus sends the response message the first apparatus via the first encrypted communication channel;

a sixth step in which the first apparatus receives data from the second apparatus via the encrypted communication channel established between the first apparatus and the second apparatus, and sends the data to the third apparatus,

wherein the first apparatus is provided with a table including at least one connection destination permitted for the third apparatus, and the first apparatus sends information of the at least one connection destination to the third apparatus in response to receiving access from the third apparatus, and receives a connection destination from the third apparatus so as to send the connection request message destined for the second apparatus to the session management apparatus in the fourth step based on the connection destination received from the third apparatus.

46. (New) The method as claimed in claim 44, wherein the session management apparatus has information for determining whether connection is permitted between apparatuses,

when the session management apparatus receives a connection request message destined for an apparatus of a connection request destination from an apparatus of a connection request source, the session management apparatus determines whether connection between the apparatus of the connection request destination and the apparatus of the connection request source is permitted by referring to the information, and

if the connection is permitted, the session management apparatus sends the connection request message to the apparatus of the connection request destination, and if the connection

is not permitted, the session management apparatus rejects the connection without sending the connection request message to the apparatus of the connection request destination.

47. (New) The method as claimed in claim 45, wherein the session management apparatus has information for determining whether connection is permitted between apparatuses,

when the session management apparatus receives a connection request message destined for an apparatus of a connection request destination from an apparatus of a connection request source, the session management apparatus determines whether connection between the apparatus of the connection request destination and the apparatus of the connection request source is permitted by referring to the information, and

if the connection is permitted, the session management apparatus sends the connection request message to the apparatus of the connection request destination, and if the connection is not permitted, the session management apparatus rejects the connection without sending the connection request message to the apparatus of the connection request destination.

48. (New) An apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus, the apparatus comprising:

a first part configured to exchange key information for encrypted communication with the session management apparatus, perform mutual authentication with the session management apparatus so as to establish an encrypted communication channel between the apparatus and the session management apparatus;

a second part configured to send, to the session management apparatus via the encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus, and receive,

from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish an encrypted communication channel between the apparatus and the second apparatus;

a part configured to perform, after being accessed by a third apparatus, processing by the first part for establishing the encrypted communication channel between the apparatus and the session management apparatus, and processing by the second part for establishing the encrypted communication channel between the apparatus and the second apparatus, and receive data from the second apparatus via the encrypted communication channel established between the apparatus and the second apparatus, and send the data to the third apparatus;

a table including at least one connection destination permitted for the third apparatus; and

a part configured to send information of the at least one connection destination to the third apparatus in response to receiving access from the third apparatus, and receive a connection destination from the third apparatus,

wherein the second part sends the connection request message destined for the second apparatus to the session management apparatus based on the connection destination received from the third apparatus.

49. (New) An apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus, the apparatus comprising:

a first part configured to exchange key information for encrypted communication with the session management apparatus, perform mutual authentication with the session management apparatus so as to establish an encrypted communication channel between the apparatus and the session management apparatus;

a second part configured to send, to the session management apparatus via the encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus, and receive, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish an encrypted communication channel between the apparatus and the second apparatus;

a part configured to perform, after being accessed by a third apparatus, processing by the second part for establishing the encrypted communication channel between the apparatus and the second apparatus, and receive data from the second apparatus via the encrypted communication channel established between the apparatus and the second apparatus, and send the data to the third apparatus;

a table including at least one connection destination permitted for the third apparatus; and

a part configured to send information of the at least one connection destination to the third apparatus in response to receiving access from the third apparatus, and receive a connection destination from the third apparatus,

wherein the second part sends the connection request message destined for the second apparatus to the session management apparatus based on the connection destination received from the third apparatus.

50. (New) A non-transitory computer-readable medium including computer program instructions, which when executed by an apparatus, cause the apparatus to perform a method of establishing an encrypted communication channel to a second apparatus by using a session management apparatus, the method comprising:

exchanging key information for encrypted communication with the session management apparatus;

performing mutual authentication with the session management apparatus so as to establish an encrypted communication channel between the apparatus and the session management apparatus;

sending, to the session management apparatus via the encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus;

receiving, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish an encrypted communication channel between the apparatus and the second apparatus;

establishing, after being accessed by a third apparatus, the encrypted communication channel between the apparatus and the session management apparatus;

establishing the encrypted communication channel between the apparatus and the second apparatus;

receiving data from the second apparatus via the encrypted communication channel established between the apparatus and the second apparatus;

sending the data to the third apparatus;

storing at least one connection destination permitted for the third apparatus;

sending information of the at least one connection destination to the third apparatus in response to receiving access from the third apparatus;

receiving a connection destination from the third apparatus; and

sending the connection request message destined for the second apparatus to the session management apparatus based on the connection destination received from the third apparatus.

51. (New) A non-transitory computer-readable medium including computer program instructions, which when executed by an apparatus, cause the apparatus to perform a method of establishing an encrypted communication channel to a second apparatus by using a session management apparatus, the method comprising:

exchanging key information for encrypted communication with the session management apparatus;

performing mutual authentication with the session management apparatus so as to establish an encrypted communication channel between the apparatus and the session management apparatus;

sending, to the session management apparatus via the encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus;

receiving, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus to establish an encrypted communication channel between the apparatus and the second apparatus;

establishing the encrypted communication channel between the apparatus and the second apparatus;

receiving data from the second apparatus via the encrypted communication channel established between the apparatus and the second apparatus;

sending the data to the third apparatus;

storing at least one connection destination permitted for the third apparatus;

sending information of the at least one connection destination to the third apparatus in response to receiving access from the third apparatus;

receiving a connection destination from the third apparatus; and

sending the connection request message destined for the second apparatus to the session management apparatus based on the connection destination received from the third apparatus.